

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-152281

(P2002-152281A)

(43) 公開日 平成14年5月24日 (2002.5.24)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 12/66		H 0 4 L 12/66	B 5 B 0 8 5
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 8 9
	3 3 0		3 3 0 A 5 K 0 3 0
H 0 4 L 12/28		H 0 4 L 11/00	3 1 0 D 5 K 0 3 3

審査請求 未請求 請求項の数12 O L (全 13 頁)

(21) 出願番号 特願2000-341926(P2000-341926)

(22) 出願日 平成12年11月9日 (2000.11.9)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 永嶋 規充

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(72) 発明者 後沢 忍

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(74) 代理人 100102439

弁理士 宮田 金雄 (外1名)

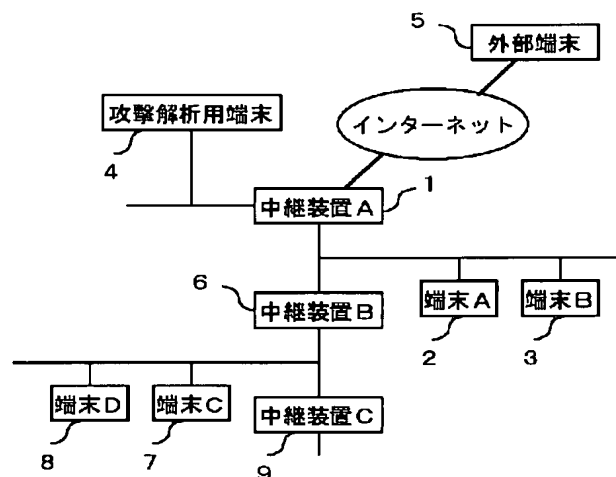
最終頁に続く

(54) 【発明の名称】 中継装置および通信システム

(57) 【要約】

【課題】 連続して不正アクセスが行われた場合の性能劣化を防ぐと共に、ネットワークに接続された端末等に不正アクセスが及ぶのを防ぐようにする。

【解決手段】 複数の端末に接続され、外部端末と上記複数の端末との通信を中継するものにおいて、複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備える。



1

【特許請求の範囲】

【請求項 1】 複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置において、

上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、

上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備えたことを特徴とする中継装置。

【請求項 2】 上記外部端末からの不正アクセスを検出した上記複数の端末のいずれかから受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部を備えたことを特徴とする請求項 1 に記載の中継装置。

【請求項 3】 上記外部端末からの不正アクセスを検出する不正アクセス検出部と、
上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部とを備えたことを特徴とする請求項 1 に記載の中継装置。

【請求項 4】 上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセスの内容を記録可能な端末に上記通信を中継することを特徴とする請求項 1 ないし請求項 3 のいずれかに記載の中継装置。

【請求項 5】 上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記通信のアクセス先アドレスの端末として振る舞う端末に上記通信を中継することを特徴とする請求項 1 ないし請求項 4 のいずれかに記載の中継装置。

【請求項 6】 上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセスの内容を解析可能な端末に上記通信を中継することを特徴とする請求項 1 ないし請求項 5 のいずれかに記載の中継装置。

2

【請求項 7】 複数の端末と、当該複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置とを備えた通信システムにおいて、

上記中継装置は、

上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、

上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備えたことを特徴とする通信システム。

【請求項 8】 上記端末は、上記外部端末からの不正アクセスを検出し、当該不正検出結果を上記中継装置に通知する不正検出通知部を備え、

上記中継装置は、上記端末から受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部を備えたことを特徴とする請求項 7 に記載の通信システム。

【請求項 9】 上記中継装置は、

上記外部端末からの不正アクセスを検出する不正アクセス検出部と、

上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部とを備えたことを特徴とする請求項 7 に記載の通信システム。

【請求項 10】 上記複数の端末のいずれか 1 つ以上の端末は、上記不正アクセスの内容を記録する不正アクセス記録部を備え、

上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致の場合に、上記不正アクセス記録部を備えた端末に上記通信を中継することを特徴とする請求項 7 ないし請求項 8 のいずれかに記載の通信システム。

【請求項 11】 上記複数の端末のいずれか 1 つ以上の端末は、上記中継装置の通信制御テーブルに登録されたアクセス先アドレスの端末として振る舞うように構成され、

上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセ

3

ス先アドレス及びアクセス元アドレスとが一致する場合に、上記中継装置の通信制御テーブルに登録されたアクセス先アドレスの端末として振る舞うよう端末に上記通信を中継することを特徴とする請求項7ないし請求項9のいずれかに記載の通信システム。

【請求項12】 上記複数の端末のいずれか1つ以上の端末は、上記不正アクセスの内容を解析する不正アクセス解析部を備え、

上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセス解析部を備えた端末に上記通信を中継することを特徴とする請求項7ないし請求項11のいずれかに記載の中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、複数の端末に接続され当該複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置と、上記複数の端末および上記中継装置を備えた通信システムとに関するものである。

【0002】

【従来の技術】 近年、インターネットの普及により、企業ネットワークをインターネットに接続するケースが多く見られる。企業ネットワークをインターネットに接続する場合、悪意のあるユーザ（クラッカーと呼ぶ）が企業ネットワークに不正にアクセスし、機密情報の漏洩、情報の改ざんが問題になってきている。

【0003】 従来、このような特定の者以外の不正アクセス者による不正アクセスや機密情報の漏洩等を防止するものとして、特開2000-47987号公報に記載されたデータ出力装置がある。

【0004】 図12は、上記データ出力装置の構成を示す構成図である。図12において、データ出力装置50は、端末57から識別情報を取得する識別情報取得手段51と、上記識別情報に基づいてその識別情報に対応する正規データの出力を許容するか否かを判断する判断手段54と、正規データを蓄積した正規データベース55と、上記正規データを出力する正規データ出力手段52と、疑似データを蓄積した疑似データベース56と、上記疑似データを出力する疑似データ出力手段53とで構成されている。

【0005】 上記のように構成されたデータ出力装置50は、端末57から取得した識別情報が正規のものであるか否かを判断手段54において判断し、正規のものである場合には、正規データベース55から正規データを読み出して正規データ出力手段52より正規データを端末57に出力する。識別情報が正規のものでない場合には、正規データとは異なる疑似データを疑似データベ

4

ス56から読み出して疑似データ出力手段53より疑似データを端末57に出力する。

【0006】 このようにして上記データ出力装置50は、不正アクセス者をあたかもアクセスに成功して正規データを手にしたかのような錯覚に陥らせ、不正アクセス者にアクセス失敗を悟られることなく、正規データの流出や、識別情報の解析等の不正行為を防止する。

【0007】

【発明が解決しようとする課題】 しかしながら、従来のデータ出力装置では、データ出力装置へ連続して不正アクセスがあった場合に、それぞれのアクセスに対して疑似データを出力する必要がある。したがって、この間に正規ユーザからアクセスがあった場合に、正規データの出力が遅れ、性能劣化をまねく問題があった。また、ネットワークに接続されているすべてのデータ出力装置に対して同様の不正アクセスが行われる可能性があり、セキュリティ上問題があった。

【0008】 本発明は、このような問題を解決するためになされたもので、連続して不正アクセスが行われた場合の性能劣化を防ぐと共に、ネットワークに接続された端末等に不正アクセスが及ぶのを防ぐことを目的としている。

【0009】

【課題を解決するための手段】 この発明に係る中継装置は、複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継するものであって、上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）が登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）と異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）の端末に上記通信を中継する中継制御部とを備えたものである。

【0010】 次の発明に係る中継装置は、上記外部端末からの不正アクセスを検出した上記複数の端末のいずれかから受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記通信制御テーブルに登録する不正アクセス登録部を備えたものである。

【0011】 次の発明に係る中継装置は、上記外部端末からの不正アクセスを検出する不正アクセス検出部と、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス（宛先アドレス）及び

アクセス元アドレス（送信元アドレス）を上記通信制御テーブルに登録する不正アクセス登録部とを備えたものである。

【0012】次の発明に係る中継装置は、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記不正アクセスの内容を記録可能な端末に上記通信を中継するものである。

【0013】次の発明に係る中継装置は、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記通信のアクセス先アドレス（宛先アドレス）の端末として振る舞う端末に上記通信を中継するものである。

【0014】次の発明に係る中継装置は、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記不正アクセスの内容を解析可能な端末に上記通信を中継するものである。

【0015】また、次の発明に係る通信システムは、複数の端末と、当該複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置とを備えたものであって、上記中継装置は、上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）が登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）と異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）の端末に上記通信を中継する中継制御部とを備えたものである。

【0016】次の発明に係る通信システムは、上記端末は、上記外部端末からの不正アクセスを検出し、当該不正検出結果を上記中継装置に通知する不正検出通知部を備え、上記中継装置は、上記端末から受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレ

ス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記通信制御テーブルに登録する不正アクセス登録部を備えたものである。

【0017】次の発明に係る通信システムは、上記中継装置は、上記外部端末からの不正アクセスを検出する不正アクセス検出部と、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記通信制御テーブルに登録する不正アクセス登録部とを備えたものである。

【0018】次の発明に係る通信システムは、上記複数の端末のいずれか1つ以上の端末は、上記不正アクセスの内容を記録する不正アクセス記録部を備え、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記不正アクセス記録部を備えた端末に上記通信を中継するものである。

【0019】次の発明に係る通信システムは、上記複数の端末のいずれか1つ以上の端末は、上記中継装置の通信制御テーブルに登録されたアクセス先アドレス（宛先アドレス）の端末として振る舞うように構成され、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記中継装置の通信制御テーブルに登録されたアクセス先アドレス（宛先アドレス）の端末として振る舞うよう端末に上記通信を中継するものである。

【0020】次の発明に係る通信システムは、上記複数の端末のいずれか1つ以上の端末は、上記不正アクセスの内容を解析する不正アクセス解析部を備え、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とが一致する場合に、上記不正アクセス解析部を備えた端末に上記通信を中継するものである。

【0021】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかる中継装置及び通信システムの好適な実施の形態を詳細に説明する。

【0022】実施の形態1. 図1は、この発明にかかる通信システムの実施の形態1のネットワーク構成を示すネットワーク構成図である。

【0023】図1において、1は、複数の端末に接続され、当該複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置Aである。ここでは、複数の端末として、端末A2、端末B3、攻撃解析用端末4に接続されており、外部端末として、外部端末5との通信を中継する。またここでは、中継装置A1と端末2～4はローカルネットワークで接続され、中継装置A1と外部端末5はインターネットで接続されている。

【0024】6は、複数の端末に接続され、当該複数の端末以外の外部端末と上記複数の端末との通信を上記中継装置A1を経由して中継する中継装置Bである。ここでは、複数の端末として、端末C7、端末D8に接続されており、外部端末として、外部端末5との通信を上記中継装置A1を経由して中継する。

【0025】9は、図示しない複数の端末に接続され、当該複数の端末以外の外部端末と上記複数の端末との通信を上記中継装置A1及び中継装置B1を経由して中継する中継装置Cである。

【0026】図2は、上記通信システムの機能構成の概略を示す機能構成図である。図1と同一又は相当部分に同一符号を付し、説明を省略する。また、図2は、本実施の形態に係る部分のみを示しそれ以外を省略して示す。

【0027】図2において、11は、上記複数の端末2、3のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）が登録された通信制御テーブルである。本実施の形態においては、上記アクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）に加え、さらに、不正アクセスがあった場合のアクセスの転送先アドレス（中継先アドレス）も登録されている。

【0028】12は、上記複数の端末2～4、7、8のいずれかに対する通信のアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）と上記通信制御テーブルに登録されているアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）とを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）と異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）の端末に上記通信を中継する中継制御部である。

【0029】ここでは、上記中継制御部12は、上記複数の端末のいずれかに対する通信のアクセス先アドレス（宛先アドレス）と異なる端末として、通信の不正アクセスの内容を記録、解析可能であるとともに、他の端末、例えば、端末A2、端末B3、端末C7又は端末D8として振る舞うことが可能に構成されている攻撃解析用端末4に通信を中継する。

【0030】13は、上記端末2、3、7、8から受信した不正アクセスの不正検出通知に基づいて、不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記通信制御テーブル11に登録する不正アクセス登録部である。

【0031】14、17、19は、それぞれ不正アクセスを検出する不正アクセス検出部である。

【0032】15は、上記不正アクセス検出部14、17、19で検出された不正アクセスの内容を記録する不正アクセス記録部である。

【0033】16は、上記不正アクセス記録部15に登録された不正アクセスの内容を解析する不正アクセス解析部である。

【0034】18、20は、それぞれ上記不正アクセス検出部17、19で不正アクセスが検出された場合に、不正検出通知として不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記中継装置A1に通知する不正検出通知部である。

【0035】ここで本発明においては、ある端末が別の端末にデータを送信する場合の宛先アドレスと送信元アドレスは、ある端末が別の端末にアクセスをする場合のアクセス先アドレスとアクセス元アドレスと同等として扱うこととし、これらを、アクセス先アドレス、アクセス元アドレスと称して説明する。

【0036】次に、図面を参照して動作について説明する。図3は、悪意のあるユーザが外部端末5から端末A2へ不正アクセスを実行し、上記端末A2が上記不正アクセスを検出して、中継装置A1に通知した場合の動作シーケンスである。

【0037】外部端末5が端末A2へ不正アクセスを実行すると、通信制御テーブル11に上記外部端末5の端末A2に対する不正アクセスが登録されていない場合は、上記不正アクセスのアクセスデータは中継装置A1の中継制御部11により上記中継装置A1を中継して上記端末A2へ伝送される（S1、S2）。

【0038】上記不正アクセスには、例えば、次のようなものが含まれる。

(1) 電子メールプロトコルSMTP(Simple Mail Transfer Protocol)のデバッグコマンドを使用し、端末A2のファイルに不正にアクセスすること。

(2) ポートスキャンにより不正にアクセスを試みること。

(3) guestやroot等のめばしいアカウント、パスワードを使用して端末A2にログインを試みること。

(4) 端末A2に電子メールを大量に送り付け、端末やネットワークのサービスを妨害すること。

【0039】上記端末A2では、不正アクセス検出部17が受信したアクセスデータを悪意のあるユーザからの不正アクセスがないかどうか解析する。ここでは、端末

A 2 が受信したアクセスデータは不正アクセスであるので、上記不正アクセス検出部 17 は、例えば上記 (1) ~ (3) のような不正アクセスを検出する (S 3)。上記不正アクセス検出部 17 が不正アクセスを検出すると、不正検出通知部 18 が上記不正アクセスの不正検出通知として不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記中継装置 A 1 に通知する (S 4)。

【0040】図 4 は、上記不正検出通知の一例を示す説明図である。図 4 において、31 は、不正検出通知を中継装置 A 1 に通知するための通信情報等が格納されたヘッダである。32 は、不正アクセスが行われた端末（ここでは、すなわち不正アクセスを検出した端末）のアドレスが格納された不正検出端末アドレスである。33 は、不正アクセスを実行した端末のアドレスが格納された不正アクセス元アドレスである。

【0041】上記外部端末 5 からの不正アクセスを検出した端末 A 2 では、不正検出通知部 18 が不正検出端末アドレス 22 に端末 A 2 を設定し、不正アクセス元アドレス 23 に外部端末 5 を設定し、ヘッダ 21 を付与した不正検出通知を中継装置 A 1 に送信する。

【0042】図 5 は、上記通信制御テーブル 11 の一例を示す説明図である。図 5 において、不正アクセス先アドレス 41 は、不正アクセスを受けた、すなわち本実施の形態では不正アクセスを検出した端末のアドレスを示す。不正アクセス元アドレス 42 は、不正アクセスを実行した端末のアドレスを示す。転送先 43 は、アクセスの転送先（中継先）の端末のアドレスを示す。

【0043】上記中継装置 A 1 は、上記不正検出通知を受信すると、不正アクセス登録部 13 が、上記不正検出通知に格納された不正検出端末アドレス及び不正アクセス元アドレスをそれぞれ不正アクセス先アドレス及び不正アクセス元アドレスとして、通信制御テーブル 11 に登録する (S 5)。

【0044】このようにして、中継装置 A 1 は、悪意のあるユーザが外部端末 5 を用いて端末 A 2 へ不正アクセスを実行した場合に、通信制御テーブルに不正アクセス先アドレスおよび不正アクセス元アドレスを登録する。

【0045】図 6 は、悪意のあるユーザが外部端末 5 から端末 A 2 へ不正アクセスを実行し、中継装置 A 1 が中継の経路を変更する場合の動作シーケンスである。

【0046】外部端末 5 が端末 A 2 へ不正アクセスを実行すると、まず、不正アクセスのアクセスデータは、中継装置 A 1 に伝送される (S 1)。当該中継装置 A 1 では、中継制御部 12 が上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル 11 に登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記アクセスデータのアクセス先アドレスと異なる端末として、攻撃解析用端末 4 に上記アクセスデータの中継し、一致しない

場合には上記アクセスデータのアクセス先アドレスに従ってその端末に上記アクセスデータの中継する。

【0047】ここでは、上記通信制御テーブル 11 は、図 5 に示すように登録されているとする。このとき、上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル 11 に登録されているアクセス先アドレス及びアクセス元アドレスとが一致するので、上記中継制御部 12 は、中継の経路を変更し (S 6)、上記アクセスデータを攻撃解析用端末 4 に中継する (S 7)。

【0048】上記攻撃解析用端末 4 は、上記中継装置 A 1 から送信されるすべてのアクセスデータを受信し、当該アクセスデータを解析して (S 8)、宛先、送信元、データ種別及び受信データの内容を収集する。また、上記攻撃解析用端末 4 は、外部端末 5 からのアクセスに対して端末 A 2 として振る舞い、外部端末 5 に応答する (S 9)。上記中継装置 A 1 は、上記攻撃解析用端末 4 の外部端末 5 に対する応答を上記外部端末 5 へ送信する (S 10)。

【0049】その後、上記攻撃解析用端末 4 は、上記アクセスデータの解析と応答を必要に応じて繰り返し、不正アクセスの情報を収集すると共に不正アクセスの内容を解析する。

【0050】このようにして、悪意のあるユーザが外部端末 5 から端末 A 2 へ不正アクセスを実行した場合に、中継装置 A 1 がアクセスデータの中継の経路を変更して、上記不正アクセスのアクセスデータを攻撃解析用端末 4 に転送することにより、端末 A 2 およびローカルネットワーク内の他の端末、例えば、端末 B 3 への不正アクセスを防ぐことができる。また、上記攻撃解析用端末 4 において、アクセスデータを記録、解析するため、不正アクセスの手順や発信元の特定に有効な情報を収集することができる。

【0051】以上のように本実施の形態によれば、中継制御部がアクセスデータの中継する際に、上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと、不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルとを比較して、一致する場合には上記アクセスデータのアクセス先アドレスと異なる攻撃解析用端末に上記アクセスデータの中継することにより、アクセス先アドレスの端末およびその端末に接続された他の端末への不正アクセスを防ぐことができ、セキュリティを向上させることができる。

【0052】また、上記中継制御部は、上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと、上記通信制御テーブルに登録されたアクセス先アドレス及びアクセス元アドレスとが一致する場合には上記アクセスデータのアクセス先アドレスと異なる攻撃解析用端末に上記アクセスデータの中継し、一致しない場合には

上記アクセス先アドレスに従ってアクセスデータを中継することにより、すなわち、不正アクセスの場合はそのアクセスデータを攻撃解析用端末に中継し、正規アクセスの場合はそのアクセスデータをアクセス先アドレスに従って中継することにより、正規アクセスに回答すべき端末、例えば、端末A、端末B等は、不正アクセスに回答する必要が無いので、不正アクセスに回答することによる正規アクセスへの回答の遅延等の性能劣化を防ぐことができる。

【0053】また、本実施の形態によれば、不正アクセス登録部が不正アクセスを検出した端末から受信した不正検出通知に基づいて、不正アクセスのアクセス先アドレス及びアクセス元アドレスを通信制御テーブルに登録することにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができる。

【0054】また、本実施の形態によれば、中継装置Aの中継制御部は、不正アクセスの内容を記録可能な上記不正アクセス記録部を備えた攻撃解析用端末に不正アクセスのアクセスデータを中継することにより、上記不正アクセス記録部に記録された不正アクセスの内容を後に解析等に利用することができるので、セキュリティを向上させることが可能となる。

【0055】また、本実施の形態によれば、中継装置Aの中継制御部は、不正アクセスのアクセス先アドレスの端末として振る舞うことが可能な攻撃解析用端末に不正アクセスのアクセスデータを中継することにより、不正アクセスを行った悪意のあるユーザに気づかれることなく、不正アクセスの手順や発信元の特定に有効な情報を収集することができる。

【0056】また、本実施の形態によれば、中継装置Aの中継制御部は、不正アクセスのアクセス先アドレスの端末として不正アクセスの内容を解析する不正アクセス解析部を備えた攻撃解析用端末に不正アクセスのアクセスデータを中継することにより、セキュリティを向上させることができる。

【0057】なお、本実施の形態では、1つの攻撃解析用端末に不正アクセス記録部と、不正アクセス解析部と、他の端末として振る舞う機能とを備えた場合について説明したが、これに限定されるものではなく、これらの機能をそれぞれ異なる複数の攻撃解析用端末に分散して備えるようにしても良い。

【0058】また、本実施の形態では、端末Aが上記不正アクセスを検出して、中継装置Aに通知するときに、上記端末Aは不正アクセスのアクセス先アドレスとアクセス元アドレスのみを上記中継装置Aに通知する場合について説明したが、さらに、不正アクセスの内容を上記中継装置Aを経由し攻撃解析用端末に送信するように構成しても良い。この場合、1回目の不正アクセスの内容も上記攻撃解析用端末に記録することができるので、よ

り多くの不正アクセスの情報を収集することが可能となる。

【0059】また、本実施の形態では、悪意のあるユーザが外部端末から端末Aへ不正アクセスを実行する場合について説明したが、外部端末から攻撃解析用端末へ不正アクセスを実行する場合は、攻撃解析用端末では、上記不正アクセスを検出すると、当該不正アクセスの内容を記録し、解析する。このとき上記攻撃解析用端末から中継装置Aへの不正検出通知および中継装置Aでの中継経路変更は不要となる。このように、不正アクセスの内容を記録または解析可能な端末に不正アクセスがあった場合は、その端末で不正アクセスの内容を記録し、解析し、中継装置Aへの不正検出通知および中継装置Aでの中継経路変更の処理を省略するようにしても良い。

【0060】実施の形態2。以上の実施の形態1では、端末で不正アクセスを検出するようにしたものであるが、次に、中継装置で不正アクセスを検出する場合の実施の形態2を示す。

【0061】本実施の形態における通信システムのネットワーク構成は、前述の実施の形態1と同様であり、説明を省略する。

【0062】図7は、本実施の形態における上記通信システムの機能構成の概略を示す機能構成図である。図1、図2と同一又は相当部分に同一符号を付し、説明を省略する。また、図7は、本実施の形態に係る部分のみを示しそれ以外を省略して示す。

【0063】図7において、21は、不正アクセスを検出する不正アクセス検出部である。中継装置で検出可能な不正アクセスとしては、例えば、次のようなものが含まれる。

(1) 電子メールプロトコルSMTP(Simple Mail Transfer Protocol)のデバッグコマンドを使用し、端末A2のファイルに不正にアクセスすること。

(2) ポートスキャンにより不正にアクセスを試みること。

【0064】次に、図面を参照して動作について説明する。図8は、悪意のあるユーザが外部端末5から端末A2へ上記(1)または(2)のような不正アクセスを実行し、上記中継装置A1が上記不正アクセスを検出して、通信制御テーブルに登録した場合の動作シーケンスである。

【0065】外部端末5が端末A2へ不正アクセスを実行すると、当該不正アクセスのアクセスデータは、まず、中継装置A1に伝送される(S1)。当該中継装置A1では、中継制御部12が上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル11に登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記アクセスデータのアクセス先アドレスと異なる端末として、攻撃解析用端末4に上記アクセスデータを中継し、一致

しない場合には、不正アクセス検出部 21 が不正アクセスの検出を行い、正規アクセスの場合に中継制御部 12 が上記アクセスデータのアクセス先アドレスに従ってその端末に上記アクセスデータを中継する。

【0066】ここでは、上記不正アクセス検出部 21 が、上記外部端末 5 の端末 A 2 に対する不正アクセスを検出する (S3)。上記不正アクセス検出部 21 が不正アクセスを検出すると、不正アクセス登録部 13 が、上記不正アクセスの不正アクセス先アドレス（ここでは、端末 A）及び不正アクセス元アドレス（ここでは、外部

端末）を通信制御テーブル 11 に登録する (S5)。

【0067】このようにして、中継装置 A 1 は、悪意のあるユーザが外部端末 5 を用いて端末 A 2 へ不正アクセスを実行した場合に、当該不正アクセスを検出し、通信制御テーブルに上記検出した不正アクセスの不正アクセス先アドレスおよび不正アクセス元アドレスを登録する。

【0068】不正アクセスの不正アクセス先アドレス及び不正アクセス元アドレスを通信制御テーブル 11 に登録した後に、再度、同一の不正アクセスが行われた場合の動作シーケンスは、前述の実施の形態 1 の図 6 と同様である。したがって、中継装置 A で不正アクセスを検出した場合には、不正アクセスのアクセスデータは端末 A に伝送されることが無いので、よりセキュリティを向上させることができる。

【0069】以上のように本実施の形態によれば、中継装置 A に不正アクセスを検出する不正アクセス検出部を備え、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録することにより、前述の実施の形態の効果に加え、不正アクセスのアクセスデータは不正アクセス先アドレスの端末に伝送される前に攻撃解析用端末に伝送されるので、よりセキュリティを向上させることができる。

【0070】なお、本実施の形態において、中継装置 A で不正アクセスが検出された際に、さらに、不正アクセスの内容を攻撃解析用端末に送信するように構成しても良い。この場合、1 回目の不正アクセスの内容も上記攻撃解析用端末に記録することができるので、より多くの不正アクセスの情報を収集することが可能となる。

【0071】また、本実施の形態では、攻撃解析用端末に不正アクセス検出部を備え、端末 A 及び端末 B に不正アクセス検出部と不正検出通知部とを備えた場合について説明したが、攻撃解析用端末から不正アクセス検出部を削除し、端末 A 及び端末 B から不正アクセス検出部と不正検出通知部とを削除し、中継装置 A のみで不正アクセスを検出するように構成しても良い。

【0072】実施の形態 3。以上の実施の形態では、悪意のあるユーザが外部端末から中継装置 A に接続された端末へ不正アクセスを実行するものであるが、次に、外

部端末から中継装置 B に接続された端末へ不正アクセスを実行する場合の実施の形態 3 を示す。

【0073】本実施の形態における通信システムのネットワーク構成は、前述の実施の形態 1 と同様であり、説明を省略する。

【0074】図 9 は、上記通信システムの機能構成の概略を示す機能構成図である。図 1、図 2 と同一又は相当部分に同一符号を付し、説明を省略する。また、図 9 は、本実施の形態に係る部分のみを示しそれ以外を省略して示す。

【0075】図 9 において、22、24 は、それぞれ不正アクセスを検出する不正アクセス検出部である。

【0076】23、25 は、それぞれ上記不正アクセス検出部 22、24 で不正アクセスが検出された場合に、不正検出通知として不正アクセスのアクセス先アドレス（宛先アドレス）及びアクセス元アドレス（送信元アドレス）を上記中継装置 B 6 を経由して上記中継装置 A 1 に通知する不正検出通知部である。

【0077】次に、図面を参照して動作について説明する。図 10 は、悪意のあるユーザが外部端末 5 から端末 C 7 へ不正アクセスを実行し、上記端末 C 7 が上記不正アクセスを検出して、中継装置 B 6 を経由し、中継装置 A 1 に通知した場合の動作シーケンスである。

【0078】外部端末 5 が端末 C 7 へ不正アクセスを実行すると、通信制御テーブル 11 に上記外部端末 5 の端末 C 7 に対する不正アクセスが登録されていない場合は、上記不正アクセスのアクセスデータは中継装置 A 1 および中継装置 B 6 を中継して上記端末 C 7 へ伝送される (S1、S11、S12)。

【0079】上記端末 C 7 では、不正アクセス検出部 22 が受信したアクセスデータを悪意のあるユーザからの不正アクセスがないかどうか解析する。ここでは、端末 C 7 が受信したアクセスデータは不正アクセスであるので、上記不正アクセス検出部 22 は、不正アクセスを検出する (S3)。上記不正アクセス検出部 22 が不正アクセスを検出すると、不正検出通知部 23 が上記不正アクセスの不正検出通知として不正アクセスのアクセス先アドレス（ここでは、端末 C）及びアクセス元アドレス（ここでは、外部端末）を上記中継装置 B 6 を経由して上記中継装置 A 1 に通知する (S13、S14)。

【0080】上記中継装置 A 1 は、上記不正検出通知を受信すると、不正アクセス登録部 13 が、上記不正検出通知に格納された不正アクセス先アドレス（ここでは、端末 C）及び不正アクセス元アドレス（ここでは、外部端末）を通信制御テーブル 11 に登録する (S5)。

【0081】このようにして、中継装置 A 1 は、悪意のあるユーザが外部端末 5 を用いて端末 C 7 へ不正アクセスを実行した場合に、通信制御テーブルに不正アクセス先アドレスおよび不正アクセス元アドレスを登録する。

【0082】図 11 は、悪意のあるユーザが外部端末 5

10

20

30

40

50

から端末C7へ不正アクセスを実行し、中継装置A1が中継の経路を変更する場合の動作シーケンスである。

【0083】外部端末5が端末C7へ不正アクセスを実行すると、まず、不正アクセスのアクセスデータは、中継装置A1に伝送される(S1)。当該中継装置A1では、中継制御部12が上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル11に登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記アクセスデータのアクセス先アドレスと異なる端末として、攻撃解析用端末4に上記アクセスデータを中継し、一致しない場合には上記アクセスデータのアクセス先アドレスに従ってその端末に上記アクセスデータを中継する。

【0084】ここでは、上記通信制御テーブル11は、不正アクセス先アドレス41に端末C、不正アクセス元アドレス42に外部端末、転送先43に攻撃解析用端末が登録されているとする。このとき、上記アクセスデータのアクセス先アドレス及びアクセス元アドレスと通信制御テーブル11に登録されているアクセス先アドレス及びアクセス元アドレスとが一致するので、上記中継制御部12は、中継の経路を変更し(S6)、上記アクセスデータを攻撃解析用端末4に中継する(S7)。

【0085】上記攻撃解析用端末4は、上記中継装置A1から送信されるすべてのアクセスデータを受信し、当該アクセスデータを解析して(S8)、宛先、送信元、データ種別及び受信データの内容を収集する。また、上記攻撃解析用端末4は、外部端末5からのアクセスに対して端末C7として振る舞い、外部端末5に応答する

(S9)。上記中継装置A1は、上記攻撃解析用端末4の外部端末5に対する応答を上記外部端末5へ送信する(S10)。

【0086】その後、上記攻撃解析用端末4は、上記アクセスデータの解析と応答を必要に応じて繰り返し、不正アクセスの情報を収集すると共に不正アクセスの内容を解析する。

【0087】このようにして、悪意のあるユーザが外部端末5から端末C7へ不正アクセスを実行した場合に、中継装置A1がアクセスデータの中継の経路を変更して、上記不正アクセスのアクセスデータを攻撃解析用端末4に転送することにより、端末C7およびローカルネットワーク内の他の端末、例えば、端末A2、B3、D8への不正アクセスを防ぐことができる。特に、中継装置B6でアクセスデータの中継の経路を変更して、攻撃解析用端末4に転送するのに比較して、よりセキュリティを向上させることができる。また、上記攻撃解析用端末4において、アクセスデータを記録、解析するため、不正アクセスの手順や発信元の特定に有効な情報を収集することができる。

【0088】以上のように本実施の形態によれば、不正アクセスのアクセス先アドレスの端末に接続された中継

装置より上位の階層の中継装置が、不正アクセスのアクセスデータの中継経路を変更し、攻撃解析用端末に転送することにより、前述の実施の形態1の効果に加え、よりセキュリティを向上させることができる。

【0089】なお、本実施の形態では、1つの攻撃解析用端末に不正アクセス記録部と、不正アクセス解析部と、他の端末として振る舞う機能とを備えた場合について説明したが、これに限定されるものではなく、これらの機能をそれぞれ異なる複数の攻撃解析用端末に分散して備えるようにしても良い。

【0090】また、本実施の形態では、端末Cが上記不正アクセスを検出して、中継装置Bを経由して中継装置Aに通知するときに、上記端末Cは不正アクセスのアクセス先アドレスとアクセス元アドレスのみを上記中継装置Aに通知する場合について説明したが、さらに、不正アクセスの内容を上記中継装置Aを経由し攻撃解析用端末に送信するように構成しても良い。この場合、1回目の不正アクセスの内容も上記攻撃解析用端末に記録することができるので、より多くの不正アクセスの情報を収集することが可能となる。

【0091】

【発明の効果】以上のように本発明の中継装置によれば、複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置において、上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備えたことにより、アクセス先アドレスの端末およびその端末に接続された他の端末への不正アクセスを防ぐことができ、セキュリティを向上させることができる。また、正規アクセスに応答すべき端末は、不正アクセスに応答する必要が無いので、不正アクセスに応答することによる正規アクセスへの応答の遅延等の性能劣化を防ぐことができるという効果を奏する。

【0092】次の発明の中継装置によれば、上記外部端末からの不正アクセスを検出した上記複数の端末のいずれかから受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部を備えたことにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができるという効果を奏する。

【0093】次の発明の中継装置によれば、上記外部端末からの不正アクセスを検出する不正アクセス検出部と、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部とを備えたことにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができる上、不正アクセスのアクセスデータは不正アクセス先アドレスの端末に伝送される前に異なる端末に伝送されるので、よりセキュリティを向上させることができるという効果を奏する。

【0094】次の発明の中継装置によれば、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセスの内容を記録可能な端末に上記通信を中継することにより、上記不正アクセス記録部に記録された不正アクセスの内容を後に利用することができるという効果を奏する。

【0095】次の発明の中継装置によれば、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記通信のアクセス先アドレスの端末として振る舞う端末に上記通信を中継することにより、不正アクセスを行った悪意のあるユーザに気づかれることなく、不正アクセスの手順や発信元の特定に有効な情報を収集することができるという効果を奏する。

【0096】次の発明の中継装置によれば、上記中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセスの内容を解析可能な端末に上記通信を中継することにより、不正アクセスを解析してセキュリティを向上させることが可能となるという効果を奏する。

【0097】次の発明の通信システムによれば、複数の端末と、当該複数の端末に接続され、上記複数の端末以外の外部端末と上記複数の端末との通信を中継する中継装置とを備えた通信システムにおいて、上記中継装置は、上記複数の端末のいずれかに通信の不正アクセスが行われた際のアクセス先アドレス及びアクセス元アドレスが登録された通信制御テーブルと、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとを比較し、一致する場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスと異なる端末に上記通信を

中継し、一致しない場合には上記複数の端末のいずれかに対する通信のアクセス先アドレスの端末に上記通信を中継する中継制御部とを備えたことにより、アクセス先アドレスの端末およびその端末に接続された他の端末への不正アクセスを防ぐことができ、セキュリティを向上させることができる。また、正規アクセスに回答すべき端末は、不正アクセスに回答する必要が無いので、不正アクセスに回答することによる正規アクセスへの回答の遅延等の性能劣化を防ぐことができるという効果を奏する。

【0098】次の発明の通信システムによれば、上記端末は、上記外部端末からの不正アクセスを検出し、当該不正検出結果を上記中継装置に通知する不正検出通知部を備え、上記中継装置は、上記端末から受信した不正検出通知に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部を備えたことにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができるという効果を奏する。

【0099】次の発明の通信システムによれば、上記中継装置は、上記外部端末からの不正アクセスを検出する不正アクセス検出部と、上記不正アクセス検出部の検出結果に基づいて、上記不正アクセスのアクセス先アドレス及びアクセス元アドレスを上記通信制御テーブルに登録する不正アクセス登録部とを備えたことにより、不正アクセスの発生に応じて通信制御テーブルを更新することができ、セキュリティを向上させることができる上、不正アクセスのアクセスデータは不正アクセス先アドレスの端末に伝送される前に異なる端末に伝送されるので、よりセキュリティを向上させることができるという効果を奏する。

【0100】次の発明の通信システムによれば、上記複数の端末のいずれか1つ以上の端末は、上記不正アクセスの内容を記録する不正アクセス記録部を備え、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセス記録部を備えた端末に上記通信を中継することにより、上記不正アクセス記録部に記録された不正アクセスの内容を後に利用することができるという効果を奏する。

【0101】次の発明の通信システムによれば、上記複数の端末のいずれか1つ以上の端末は、上記中継装置の通信制御テーブルに登録されたアクセス先アドレスの端末として振る舞うように構成され、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びア

クセス元アドレスとが一致する場合に、上記中継装置の通信制御テーブルに登録されたアクセス先アドレスの端末として振る舞うよう端末に上記通信を中継することにより、不正アクセスを行った悪意のあるユーザに気づかれることなく、不正アクセスの手順や発信元の特定に有効な情報を収集することができるという効果を奏する。

【0102】次の発明の通信システムによれば、上記複数の端末のいずれか1つ以上の端末は、上記不正アクセスの内容を解析する不正アクセス解析部を備え、上記中継装置の中継制御部は、上記複数の端末のいずれかに対する通信のアクセス先アドレス及びアクセス元アドレスと上記通信制御テーブルに登録されているアクセス先アドレス及びアクセス元アドレスとが一致する場合に、上記不正アクセス解析部を備えた端末に上記通信を中継することにより、不正アクセスを解析してセキュリティを向上させることが可能となるという効果を奏する。

【図面の簡単な説明】

【図1】 実施の形態1におけるネットワーク構成を示すネットワーク構成図である。

【図2】 実施の形態1における通信システムの機能構成の概略を示す機能構成図である。

【図3】 実施の形態1において、不正アクセスを検出し、通知した場合の動作シーケンス図である。

【図4】 不正検出通知の一例を示す説明図である。

【図5】 通信制御テーブルの一例を示す説明図である。

【図6】 実施の形態1において、中継の経路を変更す

る場合の動作シーケンス図である。

【図7】 実施の形態2における通信システムの機能構成の概略を示す機能構成図である。

【図8】 実施の形態2において、不正アクセスを検出し、通信制御テーブルに登録した場合の動作シーケンス図である。

【図9】 実施の形態3における通信システムの機能構成の概略を示す機能構成図である。

【図10】 実施の形態3において、不正アクセスを検出し、通知した場合の動作シーケンス図である。

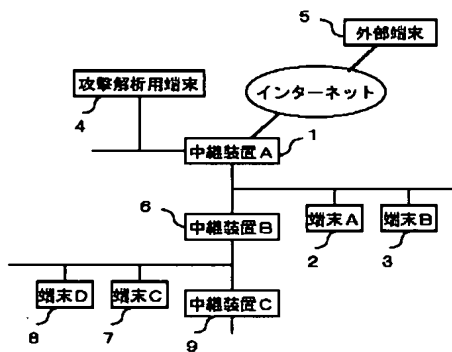
【図11】 実施の形態3において、中継の経路を変更する場合の動作シーケンス図である。

【図12】 従来のデータ出力装置の構成を示す構成図である。

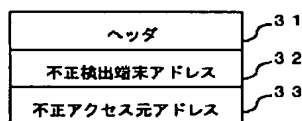
【符号の説明】

1 中継装置A、 2 端末A、 3 端末B、 4 攻撃解析用端末、 5 外部端末、 6 中継装置B、 7 端末C、 8 端末D、 9 中継装置C、 11 通信制御テーブル、 12 中継制御部、 13 不正アクセス登録部、 14、17、19、21、22、24 不正アクセス検出部、 15 不正アクセス記録部、 16 不正アクセス解析部、 18、20、23、25 不正検出通知部、 50 データ出力装置、 51 識別情報取得手段、 52 正規データ出力手段、 53 疑似データ出力手段、 54 判断手段、 55 正規データベース、 56 疑似データベース。

【図1】

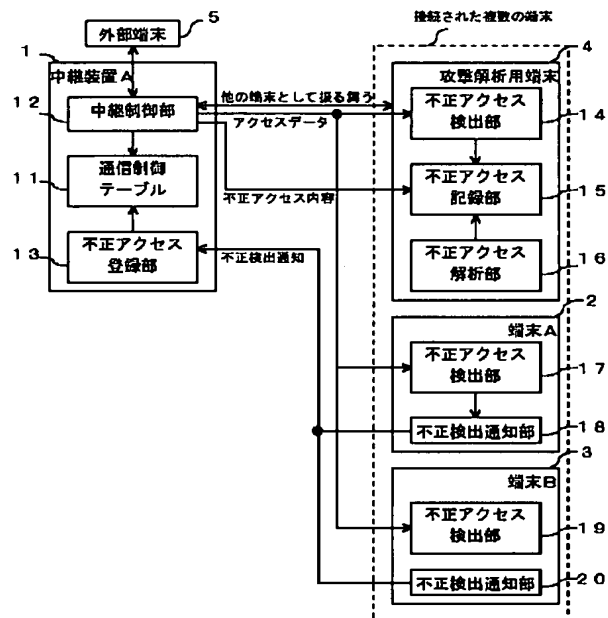


【図4】

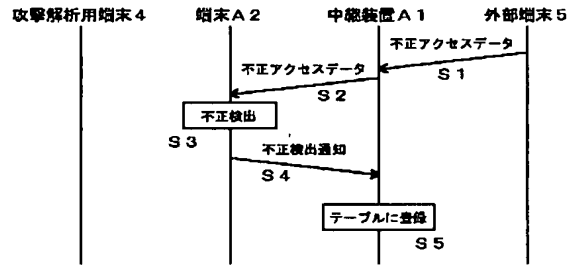


不正検出通知のフォーマット

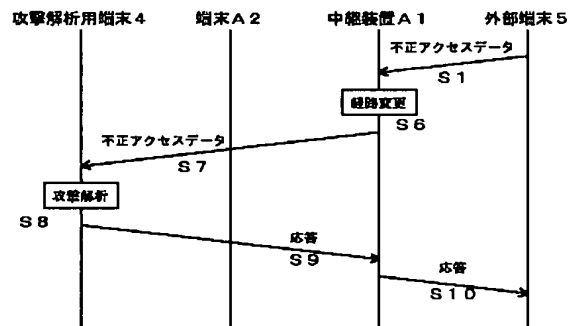
【図2】



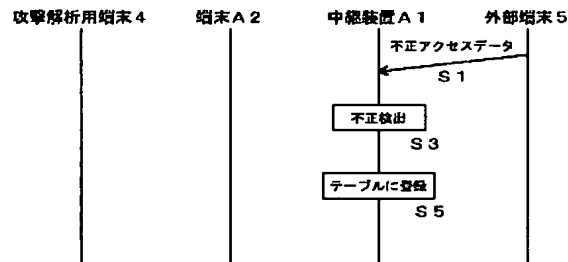
【図 3】



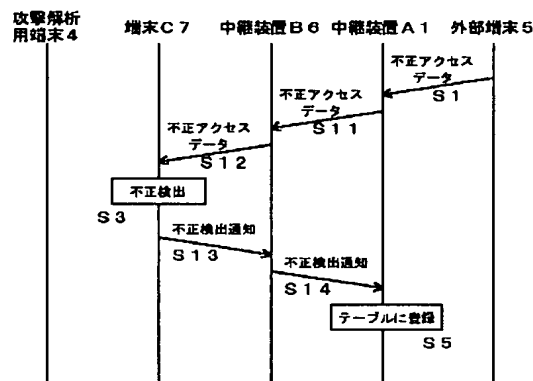
【図 6】



【図 8】



【図 10】

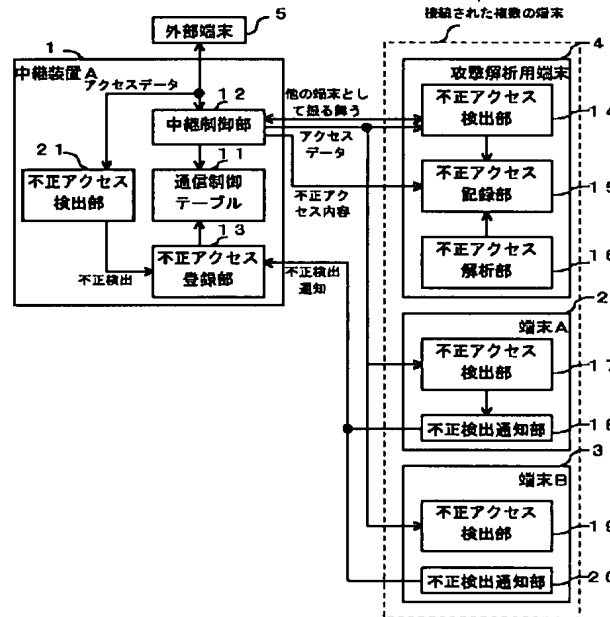


【図 5】

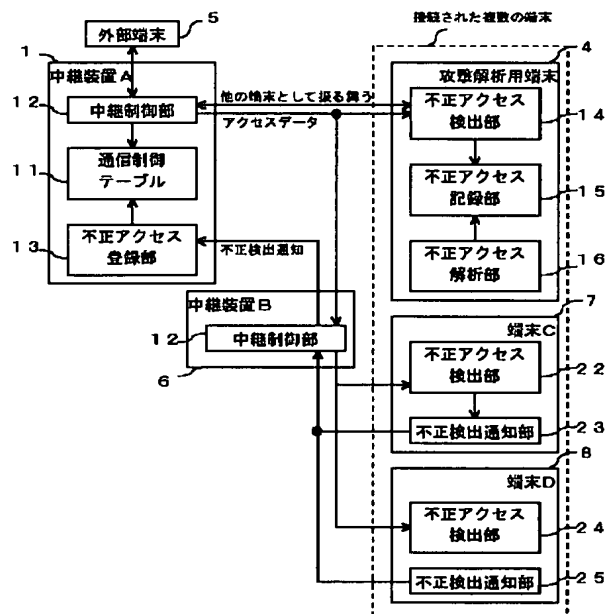
不正アクセス先アドレス	不正アクセス元アドレス	転送先
端末 A	外部端末	攻撃解析用端末
:	:	:
:	:	:

不正検出通知のフォーマット

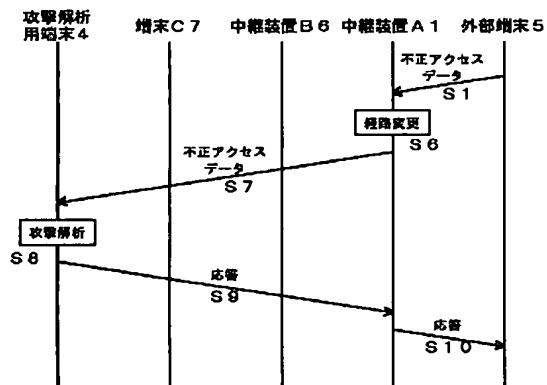
【図 7】



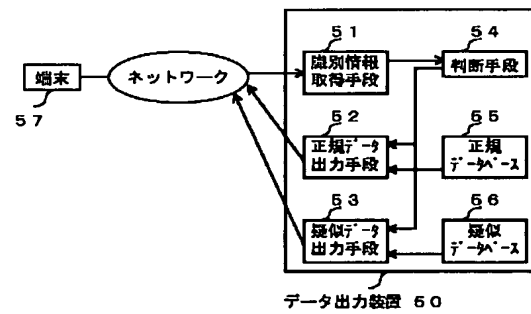
【図 9】



【☒ 1 1】



【图 1 2】



フロントページの続き

F ターム(参考) 5B085 AC03 AE01 AE06
5B089 GA21 GA31 GB02 HA10 KA17
KB13 KC34 KC52
5K030 GA15 HD03 JT02 KA04 MC08
5K033 AA08 CB08 DA01 DA06 DB18
EA06